

## PART 9—SECURITY INFORMATION REGULATIONS

### Sec.

- 9.1 Basis.
- 9.2 Objective.
- 9.3 Senior agency official.
- 9.4 Original classification.
- 9.5 Original classification authority.
- 9.6 Derivative classification.
- 9.7 Identification and marking.
- 9.8 Classification challenges.
- 9.9 Declassification and downgrading.
- 9.10 Mandatory declassification review.
- 9.11 Systematic declassification review.
- 9.12 Sharing other-agency classified information.
- 9.13 Access to classified information by historical researchers and certain former government personnel.
- 9.14 Pre-publication review of writings by former Department personnel.
- 9.15 Assistance to the Historian's Office.
- 9.16 Safeguarding.

AUTHORITY: E.O. 13526 (75 FR 707, January 5, 2010); Information Security Oversight Office Directive 32 CFR part 2001 (75 FR 37254, June 28, 2010).

SOURCE: 79 FR 35936, June 25, 2014, unless otherwise noted.

### § 9.1 Basis.

The regulations in this part, taken together with 32 CFR part 2001 and Volume 5 of the Department's Foreign Affairs Manual, provide the basis for the security classification program of the U.S. Department of State ("the Department") implementing Executive Order 13526 on Classified National Security Information ("the Executive Order" or "the Order").

### § 9.2 Objective.

The objective of the Department's classification program is to ensure that national security information is protected from unauthorized disclosure, but that it remains classified only to the extent and for such a period as is necessary.

### § 9.3 Senior agency official.

The Executive Order requires that each agency that originates or handles classified information designate a Senior Agency Official to direct and administer its information security program. The Department's senior agency official is the Under Secretary of State for Management. The Senior Agency

Official is assisted in carrying out the provisions of the Executive Order and the Department's information security program by the Assistant Secretary for Diplomatic Security, the Assistant Secretary for Administration, and the Deputy Assistant Secretary for Global Information Services.

### § 9.4 Original classification.

(a) *Definition.* Original classification is the initial determination that certain information requires protection against unauthorized disclosure in the interest of national security (*i.e.*, national defense or foreign relations of the United States), together with a designation of the level of classification.

(b) *Classification levels.* (1) Top Secret shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.

(2) Secret shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.

(3) Confidential shall be applied to information the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

(c) *Classification requirements and considerations.* (1) Information may not be considered for classification unless its unauthorized disclosure could reasonably be expected to cause identifiable or describable damage to the national security in accordance with section 1.2 of the Executive Order, and it pertains to one or more of the following:

- (i) Military plans, weapons systems, or operations;
- (ii) Foreign government information;
- (iii) Intelligence activities (including covert action), intelligence sources or methods, or cryptology;
- (iv) Foreign relations or foreign activities of the United States, including confidential sources;